**Wireshark Lab 3**

A computer screen with white text

Description automatically generated



1. Select the first UDP segment in your trace. What is the packet number[[1]](#footnote-1) of this segment in the trace file? What type of application-layer payload or protocol message is being carried in this UDP segment? Look at the details of this packet in Wireshark. How many fields there are in the UDP header? (You shouldn’t look in the textbook! Answer these questions directly from what you observe in the packet trace.) What are the names of these fields?

The packet number of the first UDP segment in the trace file is 5910, which corresponds to a DNS query sent from your device (192.168.1.47) to the DNS server (192.168.1.1) for the A record of www.nyu.edu.lan. The application-layer payload in this UDP segment is a DNS query requesting the IPv4 address for the domain. The UDP header in this packet contains four fields: Source Port, Destination Port, Length, and Checksum. These fields are visible when expanding the UDP section in the packet details of Wireshark.

1. By consulting the displayed information in Wireshark’s packet content field for this packet (or by consulting the textbook), what is the length (in bytes) of each of the UDP header fields?

The first UDP packet in the trace has the standard UDP header structure, which consists of four fields. Each field in the UDP header is 2 bytes long. These fields are SourcePort, which identifies the port number of the sender; DestinationPort, which specifies the port number of the receiver; Length, which indicates the total length of the UDP packet (header and data combined); and Checksum, used for error checking of the packet. In total, the UDP header is 8 bytes long, with each of the four fields contributing 2 bytes. These field lengths are fixed for all UDP packets, providing a consistent structure across different types of UDP communication.

1. The value in the Length field is the length of what? (You can consult the text for this answer). Verify your claim with your captured UDP packet.

The value in the Length field of the UDP header represents the totallength of the UDP packet, which includes both the UDPheader and the UDPpayload**.** This length is measured in bytes. For example, if the Length value is 75 bytes, it means the UDP packet is 75 bytes in total, with 8 bytes used for the header and the remaining bytes carrying the data (such as the DNS query or response). This field provides the full size of the UDP packet.

1. What is the maximum number of bytes that can be included in a UDP payload? (Hint: the answer to this question can be determined by your answer to 2. above)

The maximum number of bytes that can be included in a UDP payload is 65,507bytes. This is determined by the fact that the Length field in the UDP header is 2 bytes, allowing for a maximum value of 65,535 bytes. Subtracting the 8 bytes used for the UDP header, the maximum payload size is 65,535 - 8 = 65,507 bytes.

1. What is the largest possible source port number? (Hint: see the hint in 4.)

The largest possible source port number in UDP is 65,535.

1. What is the protocol number for UDP? Give your answer in decimal notation. To answer this question, you’ll need to look into the Protocol field of the IP datagram containing this UDP segment (see Figure 4.13 in the text, and the discussion of IP header fields).

The protocol number for UDP is 17 in decimal notation. This is specified in the Protocol field of the IP header, which indicates the protocol used in the payload of the IP datagram. In this case, value 17 represents UDP, as defined in the Internet Protocol standards.

1. Examine the pair of UDP packets in which your host sends the first UDP packet and the second UDP packet is a reply to this first UDP packet. (Hint: for a second packet to be sent in response to a first packet, the sender of the first packet should be the destination of the second packet). What is the packet number[[2]](#footnote-2) of the first of these two UDP segments in the trace file? What is the value in the source port field in this UDP segment? What is the value in the destination port field in this UDP segment? What is the packet number[[3]](#footnote-3) of the second of these two UDP segments in the trace file? What is the value in the source port field in this second UDP segment? What is the value in the destination port field in this second UDP segment? Describe the relationship between the port numbers in the two packets.

In the trace, the first UDP packet sent by your device is Packet 5910, where your device sends a DNS query to the DNS server. In this packet, the source port is a random port chosen by your device (e.g., 12345), and the destination port is **53**, the standard port for DNS services. The second UDP packet, which is the response from the DNS server, is Packet5911. In this packet, the source port is 53 (the DNS server's port), and the destinationport is the same as the source port of the first packet (e.g., 12345), which is your device's port. This relationship between the port numbers allows the DNS server to send the reply to the correct port on your device, ensuring the communication is correctly routed between the two devices.

1. Remember that this “packet number” is assigned by Wireshark for listing purposes only; it is NOT a packet number contained in any real packet header. [↑](#footnote-ref-1)
2. [↑](#footnote-ref-2)
3. [↑](#footnote-ref-3)